algorithms that employ elliptical curves. In accordance with the claimed subject matter, attacks against the security of the key can be thwarted by randomizing intermediate values of calculations carried out in the implementation of the algorithm, to make them unpredictable. Pursuant to the invention, the calculations are made unpredictable by choosing a random representative of a point on the elliptic curve, on which the calculation is carried out.

It is respectfully submitted that the Lopez et al. publication does not anticipate the claimed subject matter. There are a number of differences recited in the claims that are not disclosed by the reference, either explicitly or implicitly.

Selecting a random value

Claim 1 recites, as a first step, "drawing at random an integer λ such that $0<\lambda<p$", where p is a prime number. In rejecting the claim, the Office Action asserts that the Lopez publication discloses this concept, with reference to page 7, section 5.1, which states that two triplets (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) are equivalent if there exists a value λ in a finite field $GF(2^n)$ such that $X_1=\lambda X_2$, $Y_1=\lambda^2 Y_2$ and $Z_1=\lambda Z_2$. The reference does not teach, however, that the value for λ is *randomly selected*. Rather, this portion of the publication is describing a mathematical theorem, namely *if* a value for λ can be found that meets the stated condition, then the two triplets are equivalent. It does not indicate *how* the value for λ is chosen.

In particular, it does not teach that the value for λ should be a *randomly drawn integer*. This is because, unlike the claimed invention, the Lopez publication is not concerned with countermeasures against attacks on the security of cryptographic keys. It is only setting forth mathematical principles, but not teaching one how to *apply* those principles to countermeasure methods. As such, there is no need to randomly select a value for λ in the context of the Lopez publication.

Calculation of the point P'

The second step recited in claim 1 is "calculating X'1=λ^2*X1, Y'1=λ^3*Y1 and Z'1=λ*Z1 to define the coordinates of the point P'=(X'1,Y'1,Z'1)". In other words, the value X1 is multiplied by the square of λ, the value Y1 is multiplied by the cube of λ1, and the value Z1 is multiplied by λ itself, to calculate P'. With reference to this claimed subject matter, the Office Action refers to the Lopez publication's discussion of the above-noted theorem which states that $X_1=\lambda X_2$, $Y_1=\lambda^2 Y_2$ and $Z_1=\lambda Z_2$. However, this is not the *same* calculation. In particular, the elements of the triplet are not multiplied by λ^2, λ^3 and λ, respectively. Rather, two of the elements are multiplied by λ, and one of them is multiplied by λ^2. Hence, a different result would be calculated.

Calculation of the point Q

The third step of claim 1 is "calculating an output point Q=2*P' that is represented by projective coordinates (X2, Y2, Z2)". Thus, the randomly calculated point P' is used to derive the value for Q (which is used to generate the cryptographic keys). In connection with this element of the claim, the Office Action refers to page 8 of the Lopez publication, particularly its disclosure of the projective form of doubling. Again, however, it is respectfully submitted that the reference does not teach the *claimed* subject matter. It only discloses a mathematical principle, namely that projective coordinates can be doubled by means of the formula described therein. It does not disclose how to *apply* that formula as a countermeasure against attacks on the security of a cryptographic key. In particular, it does not disclose that the doubling formula should be applied to a set of projective coordinates P' that are calculated from a randomly chosen value for λ, to calculate the value for Q.

Conclusion

In summary, the Lopez publication fails to anticipate at least three elements of claim 1, namely (1) the random selection of the value for λ, (2) the calculation of a random projective point P' according to the formula set forth in the claim, and (3) the use of a random projective point P' to calculate the value for Q. It is respectfully submitted that the Lopez publication only discloses certain mathematical principles that relate to elliptic curve arithmetic. In particular, it discloses new algorithms for projective doubling and projective adding that are designed to improve the *performance* of systems that implement elliptic curve arithmetic. See sections 5.3 and 6. It does not, however, teach how to utilize those algorithms to thwart attacks on the security of cryptographic keys. Specifically, it does not disclose that the equivalence property of projective points can be used to calculate random values for the generation of cryptographic keys, to thereby make such calculations less predictable.

For at least the foregoing reasons, it is respectfully submitted that all pending claims are allowable over the prior art of record. Reconsideration and withdrawal of the rejections are respectfully requested.

Respectfully submitted,
BUCHANAN INGERSOLL PC

Date: April 3, 2006

By:
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620